УДК 004.056

И. Р. Зулькарнеев, А. Е. Козлов, А. Е. Семакин
Тюменский государственный университет, Тюмень

АВТОМАТИЗАЦИЯ ПРОЦЕССА АТТЕСТАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Аннотация. В статье рассматриваются необходимость аттестации объектов информатизации в современной России и варианты по оптимизации этого процесса для компаний-лицензиатов. Предлагается классификация анализируемой информации и дается оценка трудоемкости каждому этапа аттестации. На основе анализа данных предъявляются требования к разрабатываемому программному обеспечению по автоматизации процесса.

Ключевые слова: аттестация; автоматизация; оценка защищенности; ИСПДн; ГИС; АС.

В соответствии с действующим законодательством по защите информации, формой оценки эффективности принимаемых мер по обеспечению безопасности информации, обрабатываемой в государственных информационных системах и информационных систем персональных данных, может являться аттестация. При этом для государственных информационных систем аттестация является обязательной [1]. В среднем процедура аттестации занимает 250–300 человеко-часов, при этом бóльшую часть времени составляют сбор и анализ сведений во время предаттестационного обследования и подготовка пакета аттестационных документов, в том числе программа и методика аттестационных испытаний и протоколы аттестационных испытаний. Все это влечет существенные финансовые и временные затраты и ограничено наличием доступных человеческих ресурсов, что вынуждает компанию-лицензиата либо увеличивать штат сотрудников, либо увеличивать стоимость работ, либо уменьшать количество проектов по аттестации, либо снижать качество проведения аттестационных испытаний, тем самым повышая свои риски и уменьшая прибыль компании. Для оптимизации процесса аттестации максимизации прибыли компании-лицензиата и сокращения временных затрат можно использовать специально разработанное программное обеспечение, позволяющее автоматизировать данные процессы [2].

Для определения требований и функционала к разрабатываемому программному обеспечению необходимо оценить объем входной и анализируемой информации, трудоемкость процессов аттестации, что позволит правильно выбрать стратегию оптимизации.

При проведении аттестации объектов информатизации, которые являются автоматизированными системами различных масштабов, можно условно выделить следующие категории получаемых и обрабатываемых сведений:

1) классификационные данные об объекте информатизации (далее — ОИ):
   - тип конфиденциальной информации;
   - характеристики защищаемой информации;

2) перечень требований по защите информации при ее обработке на ОИ;

3) перечень актуальных угроз безопасности информации при ее обработке на ОИ;

4) сведения об ОИ, технических характеристиках, реализованных мерах по защите информации:
   - перечни ОТСС и ВТСС и их характеристики;
   - перечень помещений, схемы контролируемой зоны, расположения ОТСС и ВТСС;
   - перечень используемого прикладного и системного ПО;
   - меры по ограничению доступа, в том числе матрица доступа и другие организационные меры;

5) перечень организационно-распорядительной документации:
   - внутренняя документация по защите информации;
   - описание технологического процесса обработки информации;
   - технический паспорт ОИ;
   - модель угроз и нарушителя;
   - данные об используемых средствах защиты информации: наименование, версия, действующие сертификаты, формуляры, места установки;

6) данные о персонале:
   - перечень лиц, участвующих в обработке конфиденциальной информации, их уровень допуска;
   - сведения о лицах, ответственных за обеспечение безопасности информации.

Оценка трудоемкости различных этапов аттестации приведена в табл. 1 из расчета, что трудоемкость всего процесса равна 100 %.

Исходя из полученных данных видно, что существенного сокращения затрачиваемых на аттестацию ресурсов можно достичь за счет автоматизации этапов 2, 3, 4, 5, 6, 8. При этом программное обеспечение должно решать следующие проблемы:

- одновременно ведение нескольких проектов по аттестации;
- взаимодействие и импорт данных из ОИ различного масштаба, например через Active Directory;
- составление корректной модели угроз и нарушителя, учитывающей одновременно требования и ФСТЭК России, и ФСБ России [3];

– актуализация сведений в соответствии с банком данных угроз ФСТЭК России;
– определение полного перечня требований по защите информации в зависимости классификации автоматизированной системы;
– формирование и доступ к единой базе нормативно-правовых актов по защите информации, в том числе по аттестации ОИ;
– ведение перечня используемых средств защиты информации и проверка их применимости в данном ОИ;
– получение актуальных сведений из реестра ФСТЭК России о сертифицированных средствах защиты информации;
– проверка соответствия ОИ требованиям по защите информации;
– проверка целостности используемых средств защиты информации;
– выпуск пакета аттестационной документации, в том числе программы и методики аттестационных испытаний.

Таблица 1

Этапы аттестации объекта информатизации

№ п/п	Наименование этапа	Трудоемкость, %
1	Предаттестационное обследование	25
2	Оценка правильности категорирования	1
3	Определение требований по защите информации	5
4	Разработка Программы и методик аттестационных испытаний	15
5	Проведение аттестационных испытаний	20
6	Анализ организационно-распорядительной документации	10
7	Оценка уровня защищенности	10
8	Подготовка аттестационной документации	14

К сожалению, обзор существующего подобного отечественного и зарубежного программного обеспечения показал, что полноценных аналогов не существует ввиду их ограниченности по функционалу или поддержке стандартов и требований недостаточных для проведения аттестации [4]. Все это обусловливает необходимость разработки подобного программного обеспечения.

Список литературы

1. ФСТЭК России. Приказ № 17 от 11 февраля 2013 г. «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. *Барабанов А. В.*, *Марков А. С.*, *Цирлов В. Л.* Методический аппарат оценки соответствия автоматизированных систем требованиям безопасности информации // Спецтехника и связь. 2011. № 3. С. 48–52.

3. *Зулькарнеев И. Р.*, *Тякунов М. С.*, *Кибардина Ю. А.* Объединение методик создания модели нарушителя по требованиям ФСТЭК и ФСБ // Безопасность информационного пространства. Курган : РИЦ Курган. гос. ун-та, 2016. С. 22–25.

4. *Бурькова Е. В.* Задача оценки защищенности информационных систем персональных данных // Вестн. Чуваш. ун-та. 2016. № 1. С. 112–118.

УДК 004.056

Ю. А. Кибардина
Научный руководитель: ст. преп. И. И. Пряхин
Тюменский государственный университет, Тюмень

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ, НЕ ЯВЛЯЮЩЕЙСЯ ИСПДн

Аннотация. В данной работе поднимается вопрос определения уровня защищенности информационной системы, не относящейся к информационной системе персональных данных или государственной информационной системе. Рассматривается возможность применения российского и зарубежных стандартов для оценки уровня защищенности такой информационной системы.

Ключевые слова: информационная безопасность; уровень защищенности; класс защищенности; информационная система; стандарт.

При работе на предприятии или в какой-либо организации руководство может поставить перед специалистом в области информационной безопасности вопрос, насколько защищенной является наша структура. По сути, в данном случае необходимо с помощью ряда показателей оценить общий уровень защищенности информационной системы (ИС). Российские регуляторы дают четкое разграничение для оценки уровня защищенности информационной системы персональных данных (ИСПДн), а также для государственных информационных систем (ГИС), для которых предусмотрены уровни и классы защищенности соответственно. Однако бывают случаи, когда ИС не относятся ни к ИСПДн, ни к ГИС. В таком случае законодательство Российской Федерации не предлагает четкой классификации для определения защищенности ИС. Поскольку оценка уровня защищенности «произвольной ИС» (далее будем называть произвольной такую ИС, которая не относится ни к ИСПДн, ни к ГИС) производится внутренними службами, исходя из внутренних требований к информационной безопасности, выработка единой методики несколько затрудняется.